REMARKS

Claims 1-22 are pending in this application.

Rejection of Claims 1-3, 5, 7-12 and 20 under 35 U.S.C. 103(a)

Claims 1-3, 5, 7,12 and 20 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Calamera et al. (U.S. Pat. No. 6,463,533) in view of Payne et al. (U.S. Pat. No. 5,715,314). These claims are deemed to be patentable for the reasons given below. Pages 3 – 6 of the Rejection include a discussion of dependent claim 6 seemingly rejected under the above-mentioned grounds. Therefore, Applicant's response includes a discussion of rejected claim 6 despite claim 6 not appearing in the listing of rejected claims.

The present claimed invention provides a system employed by an application for encoding URL link data for use in detecting unauthorized URL modifications. A link processor processes URL data by identifying an address portion of the URL, encrypts the address portion of the URL, incorporates the encrypted address portion of the URL, together with the address portion of the URL in non-encrypted form, into a signal processed URL data string and provides a key supporting decryption of the encrypted address portion to a destination system. A communication processor incorporates the processed URL data string into formatted data for communication to the destination system. Claims 1 and 20 include similar features to those discussed above. These features are neither disclosed nor suggested by Calamera and Payne, alone or in any combination.

Calamera describes a system for allowing a computer network site to recognize an anonymous user without revealing the identity of the user. Calamera neither discloses nor suggests "encrypting said address portion of said URL" as recited in the present claimed invention. Calamera does **NOT** encrypt an address portion of a URL, but instead encrypts a URL (DOMAIN plus PATH) together with a user identification code and a random number (Calamera, column 7, lines 31-36, 42-57). This is NOT equivalent to "identifying an address portion of said URL" and "encrypting said address portion of said URL" as in the present claimed invention. In fact, Calamera, as described in column 7, line 57, uses an **irreversible** one-way hash function and does not encrypt a URL address portion.

Because Calamera does NOT encrypt an address portion of a URL, Calamera cannot disclose or suggest "incorporating said encrypted address portion of said URL,

together with said address portion of said URL in non-encrypted form, into a single processed URL data string" for encryption by a "destination system" using the provided "key supporting decryption of said encrypted address portion" as recited in the present claimed invention. Furthermore, in Calamera, "in one embodiment of the invention, a one-way hash function is used to generate a specific user alias based on the user's identification code and the URL of the website. In an alternative embodiment of the invention both a one-way hash function and a secret key encryption algorithm are used to generate the site-specific alias" (Calamera column 7, lines 1-7). Calamera generates a user specific alias code for insertion in an HTTP header in a GET request or in an HTTP GET request itself (Calamera column 12, lines 56-60, column 13, lines 17-21, Figure 7, step 126, Figure 8 step 230). Specifically,

Calamera generates the Alias code in a **first** method as: "one-way hash encryption" ALIAS = *H*(DOMAIN, PATH, ID, RANDOM)
Where: H(x) = one-way MD5 hash of ""x" and: DOMAIN = URL Internet domain name of the website being accessed PATH = URL path of the website being accessed ID = user identification code RANDOM = random data string associated with the user" (Calamera column 7 lines 42-55).

Calamera generates the Alias code in a **second** method as: ALIAS = $E[KEY_{SITE}](ID, RANDOM, CHECKSUM), DOMAIN, PATH$
Where: "secret key encryption" KEY_{SITE} = first 56 bits of: *H*(DOMAIN, PATH, KEY_{SYSTEM}) CHECKSUM = *H*(ID, RANDOM)
H(x) = one-way MD5 hash of ""x" E[k](m) = DES encryption of ""m" using secret key ""k" and: ID = user identification code KEY_{SYSTEM} = secret encryption key held by the operator of the alias server system DOMAIN = URL internet domain name of the web site being accessed PATH = URL path of the web site being accessed RANDOM = random data string associated with the user. Note that KEY_{SITE}, the encryption key used to generate the site-specific alias, is an encryption of a secret key with the URL of the website" (Calamera column 8 line 61 to column 9 line 15).

Both the first and second Calamera methods provide "a user specific alias code" for incorporation in a HTTP GET request in an encoded form. The first Calamera method provides a hashed code and the second method provides an encrypted code. However neither method shows or suggests "incorporating" an encrypted "address portion of said URL" in a URL for decryption by a "destination

system" using the provided "key supporting decryption of said encrypted address portion".

Additionally, page 4 of the Office Action admits that unlike the present claimed invention, the target system of Calamera is **unable to decrypt** (nor has access to the necessary key for decrypting) the encrypted string. Only the source (alias server) system is able to decrypt the string. This is contrary to the present claimed system wherein "a key supporting decryption of said encrypted address portion" is provided to "a destination system". Thus, Applicant respectfully submits that Calamera teaches against the present claimed system.

Payne describes a network-based sales system including at least one buyer computer for operation by a user desiring to buy a product, at least one merchant computer, and at least one payment computer. The buyer computer, the merchant computer, and the payment computer are interconnected by a computer network. Contrary to the assertion in the office action, Applicant respectfully submits that Payne (with Calamera) neither discloses nor suggests a link processor for "encrypting said address portion of said URL" as recited in the present claimed invention. Payne does NOT encrypt an address portion of a URL, but rather a **whole** URL as the encrypted URL in Payne is a hash of "other information in the payment URL", i.e., all information other than the hash value itself (see col. 7, lines 18-27). Thus, as the entire URL is encrypted by the Payne system, Payne is unable to incorporate "said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string" as recited in the present claimed invention. Further, the decryption performed by in the Payne system decrypts the entire URL and thus neither discloses not suggests "providing a key supporting decryption of said encrypted address portion, to a destination system" as recited in the present claimed invention.

Applicant further respectfully submits that contrary to the assertions in the Office Action, there is no reason or motivation to combine Calamera with Payne. Calamera and Payne are incompatible systems. Calamera is in direct conflict with the present claimed invention because Calamera teaches against conveying information in URL data fields for subsequent decryption. Additionally, Calamera is unlike the present claimed invention because the Calamera system describes that an encryption key is only held by the alias server system and cannot be used by any other system for decryption. Thus, Calamera neither discloses not suggest "providing a key supporting decryption...to a destination system" as in the present claimed invention.

Furthermore, unlike the present claimed invention, Calamera has no notion of session. Thus, the combination of Calamera with Payne would produce an inoperable system.

However, even if the combination of Calamera and Payne were able to produce an operative system, the result would be a system that uses an irreversible encryption mechanism to encrypt an entire URL and **NOT** "an address portion" as in the present claimed invention. This combination neither discloses nor suggests "encrypting said address portion of said URL" and "incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string" or "providing a key supporting decryption of said encrypted address portion, to a destination system" as recited in the present claimed invention.

Claims 2, 3, 5, 7 and 12 are dependent on independent claim 1 and are considered patentable for the reasons presented above with respect to claim 1.

With respect to claim 6, page 5 of the Office Action states, "neither Calamera nor Payne explicitly discloses converting the address portion to lower case before compression". The rejection takes Official Notice that "it is well known that addresses within URLs can be case insensitive...many hash functions, including the MD5 hash function as recited in Claim 12, by definition, are case sensitive, and will return a different result if even one input bit is changed, and certainly if a character is changed from lowercase to uppercase" (Rejection, page 5, lines 11-16). It is acceptable for official notice to be taken of a fact of "wide notoriety", In re Howard, 394 F. 2d 869, 157 USPQ 615, 616 (CCPA 1968) e.g. a fact commonly known to laymen everywhere, 29 AM. Jur 2D Evidence S. 33 (1994) or of a fact that is capable of "instant and unquestionable demonstration", In re Ahlert 424 F. 2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970). However, official notice should not be taken of a fact normally subject to the possibility of rational disagreement among reasonable men, In re Eynde, 480 F. 2d 1364, 1370; 178 USPQ 470, 474 (CCPA 1973). It is submitted that the elements of which the Rejection takes official notice, in the context of their respective claims, are neither features of "wide notoriety," (In re Howard), nor capable of "instant and unquestionable demonstration" (In re Ahlert). On the contrary, these features are subject to the possibility of rational disagreement given the claim arrangements within which they reside. Especially, given that alternative options exist such as the use of a non-case sensitive compression algorithm, for example.

Consequently, Applicants take exception to this instance of official notice used in the Rejection. Further, Applicants request that a showing be made of evidence that these features were well known, in the context of their respective claims at the time the invention was made.

Additionally, as discussed above, Applicant respectfully submits that a combination of systems as taught by Payne and Calamera would be inoperable. Specifically, Calamera uses an irreversible one-way hash function mode of encryption which is NOT ABLE to be subsequently decrypted by "a destination system". Calamera (with Payne) encrypt an entire URL. This is wholly unlike the present claimed invention which describes "encrypting said **address portion** of said URL". Therefore, it is respectfully submitted that Calamera (with Payne) fails to show or suggest "said link processor **converts** said address portion of said URL to **lower case** before compression."

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure in either Calamera et al. or Payne et al., when taken alone or in combination, that makes the present invention as claimed in claims 1 and 20 unpatentable. Applicant further respectfully submits that as claims 2-3, 5, 6, 7 and 12 are dependent on claim 1, these claims are patentable for the same reasons as claim 1. Consequently, it is respectfully submitted that this rejection is satisfied and withdrawal of the Rejection of Claims 1-3, 5, 6, 7,12 and 20 under 35 USC 103(a) is respectfully requested.

Rejection of Claim 4 under 35 U.S.C. 103(a)

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Calamera (U.S. Patent No. 6,463,533) in view of Payne (U.S. Pat. No. 5,715,314) as applied to claim 3 above, and further in view of Calow (U.S. Pat. No. 6,714,928). As claim 4 is dependent on claim 1, claim 4 is considered patentable for the reasons given above with respect to claim 1. Claim 4 is also considered patentable for the reasons given below.

Calow describes a system that provides methodologies for creating an HTML or Web database control object for use in a Client/Server Database System. Applicant

respectfully submits that Calow (with Calamera and Payne) neither discloses nor suggests "said link processor adaptively uses (a) an address portion for ASP (Active Server Page) applications comprising a SERVER_NAME and SCRIPT_NAME and (b) an address portion for a non-ASP applications comprising a SERVER_NAME, SCRIPT_NAME, and PATH_INFO" as recited in claim 4 of the present invention. While column 3, lines 49-59 of Calow describes an HTML Data Window using a component running in a transaction server cooperating with a dynamic page server (such as Microsoft Active Server Pages in IIS), there is no mention or even suggestion of the features of the present claimed invention. Rather, Calow is non-analogous art and discusses the use of Active Server Pages supporting **database application** programs (column 1, lines 20-23) and not in conjunction with "adaptively" using "an address portion," as recited in the present claimed invention.

Applicant further respectfully submits that there would be no reason or motivation to combine Calamera and Payne and Calow. As discussed above, Calamera and Payne are incompatible systems, and Calow is non-analogous art.

Thus, even if an operable system resulted from combing Calamera, Payne and Callow, Applicant respectfully submits that the combined system neither disclose nor suggest "encrypting said address portion of said URL" and "incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL string" or "providing a key supporting decryption of said encrypted address portion, to a destination system". Additionally, the references, when taken alone or in any combination, neither disclose nor suggest "said link processor **adaptively** uses (a) **an address portion** for ASP (Active Server Page) applications comprising a SERVER_NAME and SCRIPT_NAME and (b) **an address portion** for a non-ASP applications comprising a SERVER_NAME, SCRIPT_NAME, and PATH_INFO" as recited in claim 4 of the present invention.

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure in either Calamera et al., Payne et al. or Callow, when taken alone or in combination, that makes the present invention as claimed in claim 1 unpatentable. Applicant further respectfully submits that as claim 4 is dependent on claim 1, claim 4 is patentable for the same reasons as discussed above with respect to claim 1. Consequently, it is respectfully submitted that this rejection is satisfied and withdrawal of the Rejection of Claim 4 under 35 USC 103(a) is respectfully requested.

Rejection of Claims 8 and 9 under 35 U.S.C. 103(a)

Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Calamera (U.S. Patent No. 6,463,533) in view of Payne (U.S. Pat. No. 5,715,314) as applied to claim 1 above, and further in view of Levergood (U.S. Pat. No. 5,708,780). As claims 8 and 9 are dependent on claim 1, claims 8 and 9 are considered patentable for the reasons given above with respect to claim 1. Claims 8 and 9 are also considered patentable for the reasons given below.

Levergood describes a method for controlling and monitoring access to network servers. The process includes client-server sessions over the Internet involving hypertext files. When the user selects a link on a hypertext document or page that is directed to an access-controlled file, the server subjects the request to a secondary server which determines whether the client has an authorization or valid account. Upon such verification, the user is provided with a session identification which allows the user to access the requested file as well as any other files within the present protection domain. However, Levergood neither discloses nor suggests the claimed invention.

Specifically, as discussed in the Appeal Brief filed on October 12, 2005, and similarly to Calamera and Payne, Levergood neither discloses nor suggests "**encrypting** said **address portion** of said **URL** incorporating, said encrypted address portion of said URL, together with said address portion of said URL in **non-encrypted form,** into a single processed URL data string" for decryption by a "destination system" using the provided "key supporting decryption of said encrypted address portion." Levergood does not show or suggest "providing a key supporting decryption of said encrypted address portion, to a destination system," for use in decrypting the "encrypted address portion" by the "destination system" as in the present claimed invention. Applicant further respectfully re-submits arguments presented in the Appeal Brief of October 12, 2005 which are incorporated herein.

Applicant respectfully submits that contrary to the assertion on page 7 of the office action, Levergood (with Calamera and Payne) neither discloses nor suggests

"said link processor incorporates at least one of, (a) a session identifier, identifying a particular session of user initiated operation of said application and (b) an encrypted patient identifier, into said processed URL data string" as recited in claim 8 of the present invention. Nor does Levergood (with Calamera and Payne) disclose or suggest "said link processor incorporates said session identifier into said processed URL data string by formatting said session identifier into a data field including said session identifier and encrypted address separated by a colon (that is, session identifier:encrypted address)" as recited in claim 9 of the present invention. Levergood merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood states "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers" (Levergood, column 5 lines 61-65, also see column 3 lines 33-37). Neither a session identifier nor an IP address as used in Levergood is a "URL address portion" as in the present claimed invention. Levergood does NOT encrypt an address portion of a URL, as provided in the present claimed invention.

Applicant respectfully submits that as stated above with respect to claim 1, there is no reason or motivation to combine Calamera with Payne, as they are incompatible systems that teach away from each other. Similarly, Levergood and Calamera are also incompatible systems and thus cannot be combined to produce an operable system. Calamera teaches against conveying information in URL data fields for subsequent decryption in direct conflict with the encryption system of Levergood. Calamera states that the user's identity is NOT revealed (see col. 3, lines 6 – 9) and teaches that the encryption key is only held by the alias server system and cannot be used by any other system for decryption. Furthermore, unlike the present claimed invention, Calamera has no notion of session.

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure in either Calamera et al., Payne et al. or Levergood, when taken alone or in combination, that makes the present invention as claimed in claim 1 unpatentable. Applicant further respectfully submits that as claims 8 and 9 are dependent on claim 1, claims 8 and 9 are patentable for the same reasons as discussed above with respect to claim 1. Consequently, it is respectfully submitted

that this rejection is satisfied and withdrawal of the Rejection of claims 8 and 9 under 35 USC 103(a) is respectfully requested.

Rejection of Claims 13 and 14 under 35 U.S.C. 103(a)

Claims 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Calamera (U.S. Patent No. 6,463,533) in view of Levergood (U.S. Pat. No. 5,708,780). Claims 13 and 14 are considered patentable for the reasons given below.

Applicant respectfully submits that Calamera (with Levergood) neither discloses nor suggests "a link processor for processing URL data by identifying an address portion of said URL, encrypting said address portion of said URL, incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form" as recited in claim 13 of the present invention. As described above with respect to claim 1, Calamera does NOT encrypt an address portion of a URL but a URL (domain plus path) together with a user identification code and a random number (column 7, lines 31-36, 42-57). Calamera uses an irreversible one-way hash function and does not encrypt a URL address portion (column 7, line 57).

While page 8 of the Office Action states that Calamera "does not explicitly disclose the use of a session identifier," Applicant respectfully submits that Levergood also neither discloses nor suggests "incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form and a session identifier identifying a user session of computer operation, into a single processed URL data string" as recited in claim 13 of the present invention. Rather, Levergood, as described above with respect to claims 8 and 9, merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood states "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers" (Levergood, column 5 lines 61-65, also see column 3 lines 33-37).

Further, although in Levergood a valid session identifier "typically comprises" an "accessible domain" in the "SID encrypted with a secret key," the Levergood accessible domain is NOT a URL or an address portion of a URL (Levergood et al.,

column 3 lines 33-37). Levergood explicitly defines an accessible "domain" as a collection of files and NOT a URL or address portion of a URL ("A protection domain is **defined** by the service provider and is a **collection of controlled files** of common protection within one or more servers" – Levergood, column 3 lines 52-55). This is further made clear in column 5 lines 54-61 stating a "preferred SID is a sixteen character ASCII string that encodes **96** bits of SID data" that contains "an **8**-bit **domain** comprising **a set of information files** to which the current SID authorizes access." Such an "accessible domain" as used by Levergood is not in a URL link address portion. This is further corroborated in column 6 lines 29-34 of Levergood indicating that a domain is in the non-address, URL data field portion of a URL (e.g. after the question mark), specifically, a "REDIRECT URL might be: "http://auth.com/authenticate?**domain**= [domain]& URL = http://content.com/report."

Further, the purpose of the Levergood encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood column 3 lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11, lines 1-9). Consequently, there is no reason, problem recognition or motivation for amending the Levergood system to include the claimed arrangement.

It is also respectfully submitted that Levergood and Calamera are incompatible because Calamera teaches against conveying information in URL fields for subsequent decryption, as shown for example in column 3, lines 6-9, where it is stated that the user's identity is not revealed. Thus, Calamera is in direct conflict with the system described by Levergood. Additionally, Calamera provides no 35 USC 112 compliant enabling disclosure of "session" information.

Applicant further respectfully submits that even if the references were combined, a combination of Calamera with Levergood would not produce the present claimed invention. Rather, the combined system would use an irreversible encryption mechanism to ensure the validity of session identifiers. This is wholly unlike the present claimed invention wherein "a link processor for processing URL data by

identifying an address portion of said URL, encrypting said address portion of said URL, incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form." Consequently, withdrawal of the rejection of claim 13 under 35 U.S.C 103(a) is respectfully requested.

Applicant further respectfully submits that claim 14 is considered patentable for the reasons given in connected on claim 13, from which it depends. Claim 14 is also considered patentable because Calamera and Levergood, alone or in combination neither disclose nor suggest "said link processor compresses said identified address portion and encrypts said compressed address portion of said URL to provide said encrypted address portion and said link processor **converts** said identified address portion to **lower case** prior to compressing said identified address portion using a hash function" as recited in the present claimed invention. However, the Rejection takes Official Notice that "URLs are case sensitive," that a "hash function" is sensitive to uppercase and lower case characters and that as a result "forcing all characters" to lower case in the context of the claimed arrangement of claim 14 would have been obvious (Rejection page 8, line 18 to page 9, line 4). It is acceptable for official notice to be taken of a fact of "wide notoriety", In re Howard, 394 F. 2d 869, 157 USPQ 615, 616 (CCPA 1968) e.g. a fact commonly known to laymen everywhere, 29 AM. Jur 2D Evidence S. 33 (1994) or of a fact that is capable of "instant and unquestionable demonstration", In re Ahlert 424 F. 2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970). However, official notice should not be taken of a fact normally subject to the possibility of rational disagreement among reasonable men, In re Eynde, 480 F. 2d 1364, 1370; 178 USPQ 470, 474 (CCPA 1973).

Applicant respectfully submits the elements of which the Rejection takes official notice, in the context of their respective claims, are neither features of "wide notoriety," (In re Howard), nor capable of "instant and unquestionable demonstration" (In re Ahlert). On the contrary, these features are subject to the possibility of rational disagreement given the claim arrangements within which they reside. Especially, given that alternative options exist such as the use of a non-case sensitive compression algorithm, for example. Consequently, Applicants take exception to this instance of official notice used in the Rejection. Further, Applicants request that a

showing be made of evidence that these features were well known, in the context of their respective claims at the time the invention was made.

Contrary to the present claimed invention, Levergood (with Calamera) fail to show or suggest a "link processor" that "compresses said identified address portion and encrypts said compressed address portion of said URL to provide said encrypted address portion and said link processor **converts** said identified address portion to **lower case** prior to compressing said identified address portion using a hash function." Levergood (with Calamera) also does not suggest such a feature combination for reasons given in connection with claims 1 and 13. Consequently, withdrawal of the rejection of claim 14 under 35 USC 103(a) is respectfully requested.

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure in either Calamera or Levergood, when taken alone or in combination, that makes the present invention as claimed in claim 13 unpatentable. Applicant further respectfully submits that as claim 14 is dependent on claim 13, claim 14 is patentable for the same reasons as discussed above with respect to claim 13. Consequently, it is respectfully submitted that this rejection is satisfied and withdrawal of the Rejection of claims 13 and 14 under 35 USC 103(a) is respectfully requested.

Rejection of Claims 15, 16, 18, 19, 21 and 22 under 35 U.S.C. 103(a)

Claims 15, 16, 18, 19, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne (U.S. Pat. No. 5,715,314) in view of Calamera (U.S. Patent No. 6,463,533).

Applicant respectfully submits that the arguments presented above with respect to claim 1 are applicable to claims 15, 16, 18, 19, 21 and 22. Specifically, it is respectfully submitted that the system disclosed by Payne is in direct conflict with the system disclosed by Calamera. The system disclosed by Calamera is unable to encrypt and convey information in URL data fields that are to be subsequently decrypted. Contrary to Calamera, Payne encrypts "all other information" in a URL for later decryption. Thus, the teachings of Payne render the system incompatible with the system taught by Calamera. Combining the Calamera and Payne systems, even if

it were feasible, would result in a system that uses an irreversible encryption mechanism to encrypt an entire URL, not an address portion as in the present claimed invention.

Therefore, Applicant respectfully submits that Payne (with Calamera) neither discloses nor suggests "a link processor for processing said encoded URL by identifying an encrypted **address portion of said received encoded URL** and a corresponding non-encrypted address portion of said received encoded URL, decrypting said encrypted address portion of said URL to provide a decrypted URL address portion" as recited in claims 15 and 21 of the present invention. Payne does NOT encrypt an address portion of a URL but a whole URL as it is a hash of "other information in the payment URL" (i.e., all information other than the hash value itself, column 7, lines 18-27). Additionally, Calamera (with Payne) merely encrypts a URL (domain plus path) together with a use identification code and a random number, as opposed to encrypting an "address portion of a URL," as recited in the present claimed invention (Calamera column 87, lines 31-36, 42-57). Calamera uses an irreversible one-way hash function and does not encrypt a URL address portion (column 7, line 57).

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure in either Payne or Calamera, when taken alone or in combination, that makes the present invention as claimed 15 and 21 unpatentable. Applicant respectfully submits that as claims 16, 18 and 19 are dependent on claim 15 and claim 22 is dependent on claim 21, claims 16, 18, 19 and 21 are patentable for the same reasons as claims 15 and 21, respectively. Consequently, it is respectfully submitted that this rejection is satisfied and withdrawal of the Rejection of Claims 15, 16, 18, 19, 21 and 22 under 35 USC 103(a) is respectfully requested.

Rejection of Claim 17 under 35 U.S.C. 103(a)

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Payne (U.S. Pat. No. 5,715,314) in view of Calamera (U.S. Patent No. 6,463,533) as applied to claim 15 above, and further in view of Levergood (U.S. Pat. No. 5,708,780). Claim 17 is dependent on claim 15 and is considered to patentable for the reasons given in connection with claim 15 as well as the reasons given below.

Applicant respectfully submits that Levergood (with Calamera and Payne) neither disclose nor suggest "said link processor identifies and extracts a session identifier from a non-encrypted portion of said received encoded URL" as recited in claim 17 of the present invention. Neither a session identifier nor an IP address as used in Levergood, is a "URL or URL address portion" as in the present claimed invention. Levergood does not encrypt an address portion of a URL, as recited in the present claimed invention. The Levergood digital signature comparison relied on in column 6, lines 5-16 is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood column 3, lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11, lines 1-9).

As described above with respect to claim 1, there is no reason, problem recognition or motivation for combining Payne and Calamera as they are incompatible systems. There is also no reason or motivation for adding the Levergood system to this incompatible mix. Specifically, Calamera provides no 35 USC 112 compliant disclosure regarding session information as in the present claimed invention. Furthermore, unlike the present claimed invention, Calamera teaches against subsequent decryption of URL data fields by a destination system. Thus, the combination of Payne, Calamera and Levergood would produce an inoperative system. Consequently, Applicant respectfully submits that Payne, Calamera and Levergood, alone or in any combination, neither disclose nor suggest that "said link processor identifies and extracts a session identifier from a non-encrypted portion of said received encoded URL" as recited in the present claimed invention. Thus, withdrawal of the rejection of claim 17 under 35 USC 103(a) is respectfully requested.

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure in either Payne, Calamera or Levergood, when taken alone or in combination, that makes the present invention as claimed in claim 15 unpatentable. Applicant respectfully submits that as claim 17 is dependent on claim 15, claim 17 is patentable for the same reasons as claim 15. Consequently, it is respectfully submitted that this rejection is satisfied and withdrawal of the Rejection of claims 17 under 35 USC 103(a) is respectfully requested.

A Supplemental Information Disclosure Statement was filed on May 1, 2006 identifying U.S. Patent No. 6,971,067; 6,941,313 and 6,993,556 for consideration. Applicant respectfully submits that these Patents neither disclose nor suggest the present invention as claimed in claims 1 – 22. Therefore, Applicant further respectfully submits that systems disclosed in these patents provide no 35 USC 112 compliant enabling disclosure that would make the present claimed invention unpatentable.

In view of the above amendments and remarks, Applicants submit that the Application is in condition for allowance, and favorable reconsideration is requested.

Respectfully submitted,

Date: June 12, 2006

Alexander J. Burke
Reg. No. 40,425

Alexander J. Burke
Intellectual Property Department
Siemens Corporation,
170 Wood Avenue South
Iselin, N.J. 08830
Tel. 732 321 3023
Fax 732 321 3030